STATEWIDE GUIDELINES FOR IMPLEMENTATION OF INFORMATION SYSTEM SECURITY

Statewide Guidelines: Information Systems Security

Effective Date: August 8, 2008

Approved: State of Montana Chief Information Officer

Replaces & Supercedes: None

I. Purpose

The purpose of these guidelines is to describe for all state agencies the framework for development of a comprehensive, collaborative security program to ensure the integrity, availability, and confidentiality of state information systems ("IS") and the data contained in those systems, and to identify the anticipated timeframes for implementation of statewide IS security policies to implement the overall IS security program. The primary objectives of the overall IS security program are to: identify the applicable IS security standards for the State of Montana; develop an appropriate infrastructure for security management; conduct security awareness training; conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and controls; develop a process for planning, implementing, evaluating, and documenting remedial actions; develop procedures for detecting, reporting, and responding to security incidents.

These guidelines will assist information security stakeholders (agency heads, chief information officers, agency information security officers, and security managers) in planning, both through the budget process and through personnel development, for implementation of the IS security program by providing a detailed roadmap of anticipated security policy implementation.

To the extent applicable, these guidelines and all subsequently issued policies will apply to any entity utilizing the state IS network.

II. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. §2-17-505(1), MCA. It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the

state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. §2-17-505(2), MCA.

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. §2-17-512, MCA.

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. §2-15-114, MCA.

III. Announcement of Security Standards

DOA hereby announces that it will work to the security standards established by the National Institute of Standards and Technology ("NIST") in establishing and enforcing statewide information technology policies and standards. DOA may vary, modify, or selectively apply the NIST standards to be implemented in statewide policies and standards if, in the DOA's judgment, the variance, modification, or selective application of those standards is in the best interests of the state of Montana. The DOA may also grant a state agency an exception to application of a specific policy, standard, or other requirement, in conformity with §2-17-515, MCA, if such exception is in the best interests of the state of Montana.

IV. Effective Date of Security Standards

DOA will implement the overall security program through the adoption and issuance of security policies. The issuance of specific policies is anticipated to occur in the timeframes outlined in Exhibit A to these guidelines. Each policy issued will include information regarding staffing, hardware, software, or other resources required for compliance, and identify an effective date that provides a sufficient time for implementation, taking into account budgeting and legislative timelines.

In the interim, state agencies must continue to give effect to any currently-in-force policies, standards, or other requirements pertaining to security of state information systems and the information contained in them.

V. Agency Staffing for IS Security Purposes

Each state agency will need to have competent staff assigned for the following functions in order to insure appropriate implementation and ongoing management of the IS security program. An agency will be authorized to assign staff in a manner consistent with its size, complexity, and financial capabilities, including that IS Security staff may be obtained through contracted IS service providers.

Information Security Officer (ISO): The ISO will have overall responsibility for ensuring the agency's compliance with the IS security program, policies, and standards. The ISO will be the primary point of contact with DOA's Information Technology Services Division (ITSD); will ensure agency staff are appropriately educated regarding IS security policies, standards, and practices; and will investigate and address actual and suspected IS security threats and violations within the agency.

VI. Information System Requirements – Hardware/Software

State agencies may be required to purchase, update, or supplement hardware and/or software assets in order to achieve the necessary technological capacity to comply with specific policies or standards. Where necessary, minimum hardware/software specifications will be identified in issued policies and standards.

VII. Education

ITSD will develop a training and awareness program that will include responsibilities of technical staff, business process and information proponents, strategic business planners, and users. ITSD will make this training available to assist agencies in the implementation of individual IS policies and the overall IS program.

VIII. Close

For questions or comments about this instrument, contact the Information Technology Services Division at ITSD Service Desk, or:

PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IX. Cross-Reference Guide

A. State/Federal Laws/MOM

- 2-15-114. Security Responsibilities Of Departments For Data
- MOM 3-0130 Discipline

B. IT Procedures or Guidelines Supporting this Policy

- Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards
- NIST Special Publications (800 Series)
- FIPS Publications

X. Administrative Use

Product ID:	GDL-20080101a
Proponent:	State of Montana Chief Information Officer
Version:	1.0
Approved Date:	August 7, 2008
Effective Date:	August 8, 2008
Change & Review Contact:	ITSD Service Desk
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	August 1, 2013
Last Review/Revision:	
Change Record:	

Exhibit A

Anticipated Issuance Sequence and Timeframe

Information systems security guidance shall be published based upon the National Institute of Standards and Technology defined security control families. The control family guidelines shall be published on a quarterly basis within fiscal years, until all seventeen families are published.

The projected publishing sequence is listed below, but may be affected by operational constraints/requirements or external factors. The Issuance Timeframe is the anticipated timeframe for first release of the policy/standard. The effective date of each policy/standard will be specified in the policy/standard, and will be based on the time reasonably necessary for agencies to implement the policy/standard, including any time necessary for budgeting and legislative processes if applicable.

Control Family	Target Publication Timeframe
Information Security Roles	1QFY2009
Control Family Eight - **Incident Response**	1QFY2009
Control Family Two - **Awareness and Training**	2QFY2009
Control Family Fourteen - **Risk Assessment**	3QFY2009
Control Family One - **Access Control**	4QFY2009
Control Family Sixteen - **Systems and Communications Protection**	1QFY2010
Control Family Four - **Certification, Accreditation, and Security Assessments**	2QFY2010
Control Family Seventeen - **System and Information Integrity**	3QFY2010
Control Family Twelve – **Planning**	4QFY2010

Control Family Fifteen - **System and Services Acquisition**	1QFY2011
Control Family Five - **Configuration Management**	2QFY2011
Control Family Six - **Contingency Planning**	3QFY2011
Control Family Eleven - **Physical and Environmental Protection**	4QFY2011
Control Family Ten - **Media Protection**	1QFY2012
Control Family Nine – **Maintenance**	2QFY2012
Control Family Thirteen - **Personnel Security**	3QFY2012
Control Family Seven - **Identification and Authentication**	4QFY2012
Control Family Three - **Audit and Accountability**	1QFY2013